North Dakota Homeland Security Anti-Terrorism Summary

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

Quick Links

North Dakota

Nothing Significant to Report

Regional

(Minnesota) **Telephone credit card scam targets business owners.** The Better Business Bureau said a new telephone-based scam abusing disability services is targeting many small businesses, including restaurants and other business types. In the scam, a business owner receives a call through the Telecommunications Relay Service (TRS) asking for an extremely large delivery order. After placing the order, the scammer asks if they can overpay, and have the difference sent to them. Afterwards, the credit card number is found to be stolen, leaving the company short whatever money they sent. The TRS system was designed to assist people who have hearing or speech problems. The system allows users to type what they would like to say, and a communications assistant will relay that along, and type back the response to the user. By using TRS to make the fraudulent calls, business owners never see or hear the scammer in person. Two Minnesota restaurants have already reported the scam to the BBB, which says any type of business could be vulnerable to it. Source: http://www.activefilings.com/business-formation-services/telephone-credit-card-scam-targets-business-owners/

(Montana) **Water seeping through dam at the Basin Creek Reservoir.** The recent rain combined with runoff from the Highland Mountains south of Butte, Montana has forced water to seep through the dam at the Basin Creek Reservoir. The water washed out a ditch at the site. The area dried up after the flood gates were open, the manager for water treatment for Butte-Silver Bow said. Water from the reservoir is gushing out. He said the recent rain combined with runoff brought the water level close to full pool. But once the gates were opened, the level dropped by a foot and a half within 24 hours. The integrity of the dam was never compromised, he said. However, with the gates open, the creek is running high with water flowing over this portion of the road downstream. Workers are also keeping a close eye on the culverts and said they are in good shape. The dam was built in 1890. It was inspected in 2006 and that is when a new spill wall was installed. Just east of the reservoir, city county workers were busy repairing a section of Roosevelt Drive off of Highway 2 where the stretch of road was starting to crumble into the rushing waters of Blacktail Creek. Workers were filling in the washed out section with boulders, sand and gravel. Source: http://www.kxlf.com/news/water-seeping-through-dam-at-the-basin-creek-reservoir/

(Montana) **Canyon Ferry Reservoir opens floodgates.** Water managers said above-normal precipitation has filled Canyon Ferry Reservoir in Helena, Montana to 98 percent and the floodgates have been opened to allow water over all four spillways. The reservoir and river supervisor for the Bureau of Reclamation said water at a rate of 14,700 cubic feet per second is flowing over the spillways, while water was flowing into the reservoir at 21,900 cubic feet per second. The reservoir is

considered full at an elevation of 3,797 feet, and on Friday was at 3,796.1 feet. Source: http://www.kulr8.com/news/state/96225714.html

(South Dakota) **Gavins Dam reservoir reaches record level.** The Army Corps of Engineers said it has increased releases from Gavins Point Dam near Yankton, South Dakota to prevent water from flowing over the emergency spillway gates. The move Monday night leveled the elevation of the reservoir at a record 1,209.7 feet, less than half a foot from the top of the spillway gates. Gavins Point releases were increased from 30,000 cubic feet per second (cfs) to 33,000 cfs. The Corps said releases will be held there until flooding begins to subside downstream, then might be increased to 35,000 cfs. Heavy rainfall has fallen recently in parts of the central Missouri River basin. The Corps said that with forecasts for only light rain over the next several days, the high river flows are expected to begin falling later this week. Source: http://www.ktiv.com/Global/story.asp?S=12654002

National

BP's next challenge: disposal of tainted sludge. Oil giant BP is facing a new challenge in disposing of the millions of gallons of potentially toxic oil sludge its crews are collecting from the Gulf of Mexico, according to industry experts and veterans of past spills. Crews so far have skimmed and sucked up 21.1 million gallons of oil mixed with water, according to the Deepwater Horizon Unified Command. Because the out-of-control well may continue spewing for months, that total almost certainly will surge. BP's plan for handling the gooey mess, written in conjunction with the Coast Guard, the Environmental Protection Agency and Louisiana officials, calls for reclaiming or recycling as much as possible. Some experts said that approach is the best option for the environment, but it has not worked in previous spills. It is not profitable to refine sludge that has mixed with water and seagoing debris because it can actually ruin refineries, they said. "It has no longer got any economic value. It has to be disposed of as garbage," said a former Navy officer who helped oversee numerous oil-spill cleanups, including the 1989 Exxon Valdez in Alaska. "The stuff that got recovered from the Exxon Valdez was just a nightmare." Source: http://www.usatoday.com/news/nation/2010-06-16-oil-waste_N.htm

Real-time data help inquiry into rig explosion. Unable to survey wreckage on the seafloor directly, investigators into the fatal Deepwater Horizon accident are relying on clues from what may be the next-best thing. Prior to the April 20 disaster, BP offices onshore were receiving minute-by-minute data about the company's Macondo well, transmitted by satellite, that may offer the most complete picture available of problems that led to the tragic blast and the biggest oil spill in U.S. history. Records of that information are stored with BP and Halliburton Co., the oil field services company that had a contract with BP to collect real-time data from the well and rig and send it ashore. Now, various congressional committees are sorting through it. The Coast Guard and U.S. Minerals Management Service, which have formed a joint investigation board into the incident, are also planning to discuss the data during a third round of hearings in July, a Coast Guard spokesman said. And plaintiffs' attorneys involved in suits against BP and other contractors aboard the rig are trying to obtain it and use it to bolster their cases. Major oil companies including Shell Oil, Chevron Corp. and ConocoPhillips increasingly use real-time well data to monitor offshore drilling projects, especially big and costly deep-water wells. The information allows shore-based engineers to assist during important drilling phases and intervene when problems arise. Source: http://www.chron.com/disp/story.mpl/business/7049301.html

INTERNATIONAL

Paraguyan government website hosts phishing data. Phishing gangs are growing increasingly bold, evinced by researchers finding phishing data on a Web site owned by the Paraguayan government. Sunbelt researchers discovered that a Web site belonging to the Paraguayan government is hosting data on banks and insurance companies in the United Kingdom gathered through phishing attacks. The researchers have notified the Web site owners regarding the data cache. Typically, researchers will sit on the data and try to learn more information about the cyber criminals. Hosting stolen data on another server is considerably safer for cyber criminals, and operates similar to a "slick" used by spies. The data remains accessible but if anyone stumbles upon the data, the police are unable to arrest the criminals. Source: http://www.thenewnewinternet.com/2010/06/17/paraguyan-government-website-hosts-phishing/

Shootout in Mexican tourist town of Taxco leaves 15 dead. Fifteen suspects were killed June 15 in a shootout with soldiers in the tourist town of Taxco, Mexico. A citizen's complaint about presumed illicit activities at a house led authorities to dispatch soldiers to a house in the town. Upon arriving at the house, they were greeted by gunfire and, acting in self-defense, responded with gunfire of their own. The battle continued for about 40 minutes, after which authorities determined that 15 "aggressors" were dead, and 16 long guns, six pistols, two home-made explosive devices and a vehicle were confiscated. The process of identifying the bodies was under way. Source: http://edition.cnn.com/2010/WORLD/americas/06/15/mexico.taxco.killings/?hpt=T2

50 activists arrested at Swedish nuclear plant. Swedish police on Monday arrested 50 Greenpeace activists after they broke into a nuclear power plant site to protest the country's use of atomic energy, officials said. The protesters climbed a fence of the Forsmark, Sweden power plant and were detained on suspicion of trespassing and breaking safety regulations, police spokesman said. A Greenpeace spokesman said activists from Germany, Poland and Nordic countries were demonstrating against government plans to allow the construction of new nuclear plants. Sweden's environment minister told local news agency TT that the Greenpeace action had exposed serious flaws in the safety at the Forsmark plant. "It is not acceptable that it's possible to get that close to the actual plant," he said. "The protection around Swedish nuclear plants needs to be strengthened and that responsibility lies with the reactor owners." The Swedish minister said he has demanded a report of the incident from the Swedish Radiation Safety Authority. Source: http://www.fox11az.com/news/world/96291233.html

At least 24 killed as gunmen storm Iraq's Central Bank. Armed men wearing police-commando uniforms briefly overran Iraq's Central Bank on Sunday, killing at least 24 people in a brazen daylight assault in the heart of Baghdad's busiest commercial district. The corpses of seven more men wearing uniforms and suspected of being among the assailants were found inside the bank after police finally entered, four hours after the assault began. At least 46 people were injured. Some of the casualties were civilians caught in explosions or gunfire outside the bank, and others were employees trapped inside, police said. It was the latest in a string of heists targeting banks and jewelers in Iraq, but at least one of the assailants killed himself using an explosives vest, suggesting the motive may have been sabotage rather than robbery. The assault exposed the vulnerabilities of the Central Bank, one

of Iraq's most vital institutions. Once storming two separate entrances, the gunmen apparently roamed through the building, though what exactly happened inside was still murky late in the evening. Security forces fearing a hostage scenario ringed the bank, and when they finally entered shortly after 7 p.m., they found only dead and injured bank employees and the seven bodies of suspected assailants. According to a Major General who is the spokesman for security forces in Baghdad, no apparent attempt was made to steal money, but several floors of the building were set ablaze after the gunmen entered. "They didn't steal anything," he told the state broadcaster Al Iraqiya. "Their purpose was to sabotage, and though we can't accuse anyone now, the fingerprints of Al Qaeda are very obvious." Source: http://www.latimes.com/news/nationworld/world/la-fg-iraq-bank-20100614,0,6370835.story

Banking and Finance Industry

Sophisticated ATM skimmer transmits stolen data via text message. Operating and planting an ATM skimmer — cleverly disguised technology that thieves attach to cash machines to intercept credit- and debit-card data — can be a risky venture, because the crooks have to return to the scene of the crime to retrieve their skimmers along with the purloined data. Increasingly, however, criminals are using ATM skimmers that eliminate much of that risk by relaying the information via text message. One particular craftsman, designs the fraud devices made-to-order, even requesting photos of the customer's targeted ATMs before embarking on a sale. Just as virus writers target Windows because it is the dominant operating system on the planet, skimmer makers center their designs around one or two ATM models that are broadly deployed around the globe. Among the most popular is the NCR 5886. This skimmer sells for between $7,000 and $8,000, and includes two main components: The card-skimmer device that fits over the card acceptance slot and records the data that is stored on the back of any ATM cards inserted into the device; and a metal plate with a fake PIN pad that is designed to sit directly on top of the real PIN pad and capture the victim's personal identification number (PIN) while simultaneously passing it on to the real PIN pad underneath. Not all skimmers are so pricey: Many are prefabricated, relatively simple devices that fraudsters attach to an ATM and then collect at some later point to retrieve the stolen data. Source: http://krebsonsecurity.com/2010/06/sophisticated-atm-skimmer-transmits-stolen-data-via-text-message/

Authorities reveal mortgage fraud crackdown, 485 arrests. U.S. authorities have charged 1,215 people in hundreds of mortgage fraud cases that resulted in estimated losses of $2.3 billion, top presidential administration officials said June 17, unveiling a crackdown after the housing market collapse. The administration has been under pressure to root out mortgage fraud and improve oversight of the housing market after the housing bubble touched off a global economic slide, and led to a cascade of home foreclosures in the United States. Over the last three-and-a-half months, authorities have made 485 arrests in the fraud cases, obtained 336 individual convictions and recovered more than $147 million, the Justice Department said. The announcement comes a day after U.S. prosecutors unveiled charges against the former head of a now-defunct mortgage lender for an alleged fraud scheme that led to multibillion-dollar losses. Source: http://www.reuters.com/article/idUSTRE65F3E620100617?type=domesticNews

Digital currency: "The future of goverment payments". Digital currency has the potential to dramatically transform government payments in the next five years, saving U.S. taxpayers hundreds

of millions of dollars, according to representatives from the government and private sector. The positive impact of digital currency on all aspects of government payments and purchasing was highlighted at a June 16 briefing in Washington, D.C. Speakers at the event, including Visa's global head of corporate relations, pointed to plans by state, local and federal government agencies to launch or expand electronic-payment programs to improve efficiency, accountability and transparency. "Switching from inefficient paper processes to digital currency can have a sizable long-term impact," he said. Among the expected future savings cited at the event: The U.S. Department of Treasury has announced plans to switch to electronic payments, eliminating about 136 million paper checks, saving almost $50 million in postage and $300 million over the first five years; The U.S. Social Security Administration and U.S. Department of Veterans Affairs have announced the completion of the switch to digital currency for benefits payments. Treasury reported that while it costs about $1 to print and mail a check, each digital-currency payment cost 10 cents. Currently, 39 states deliver benefits on Visa prepaid cards to recipients of 71 programs for child support, unemployment insurance and Temporary Assistance for Needy Families disbursements. Some states have realized savings that have reduced the cost of distributing benefits dramatically. Nebraska, for example, used to pay 59 cents to print and mail each check, but pays only about one penny to reload a prepaid card. Finally, the U.S. General Services Administration's SmartPay program provides purchase, travel, fleet and integrated payment card programs to more than 350 federal agencies and departments, saving these agencies $1.7 billion — up to $70 per purchase, according to the GAO. Source: http://www.marketwatch.com/story/digital-currency-the-future-of-government-payments-2010-06-15?reflink=MW_news_stmp

New tab napping scam targets your bank information. Tab napping is more sophisticated than phishing scams and doesn't rely on persuading a user to click on a link to a scammer's Web page. Instead, it targets Internet users who open lots of tabs on their browser at the same time. It works by replacing an inactive browser tab with a fake page set up specifically to obtain personal data - without the user even realizing it has happened. So, it is not safe to assume that after a user has opened a new tab and visited a Web page, that the Web page will stay the same even if the user does not return to it for a time while using other windows and tabs. Malicious code can replace the Web page a user opened with a fake version which looks virtually identical to the legitimate page one originally visited. Users can guard against tab napping by keeping a close eye on tabs they open. Make sure the URL in the browser address page is correct before entering log-in details. A fake tabbed page will have a different URL to the Web site one thinks she is using. Always check that the URL has a secure https:// address even if tabs are not open on the browser. Source: http://www.bbb.org/us/post/new-tab-napping-scam-targets-your-bank-information-3813

Development of call protection could lead to the end of the theft of customer payment data exchanged over the telephone. Ten major audio data thefts that have occurred in the last year have led to the development of a device that detects and blocks the "DTMF" (dual-tone multi-frequency signaling) tones and obscures card details. Set to be released in less than two months by British company Veritape, "CallGuard" solves a technical problem for call centers that has appeared to be near insurmountable until now. The company claimed that the theft of customer payment data exchanged over the telephone could be eliminated, particularly as a recent study by Veritape identified 93 percent non-compliance to payment data regulations amongst UK call centers due to the complexity and cost of compliance. The managing director of Veritape said that industry rules make protection and non-storage of credit card details a mandatory requirement for call centers, but

despite this, most call centers are in breach of the guidelines. According to Veritape, CallGuard is fully compatible with any call-recording system and ensures that recorded telephone conversations are fully compliant with the PCI DSS regulations. It works by detecting and blocking "DTMF" tones, the sounds produced when keying in a number. By doing this it prevents any storage of the numbers communicated by the customer. At the same time it automatically enters card details into password style fields, which themselves are obscured with asterisks. The technology is built into a box the size of a large shoebox with an additional small USB device per workstation. It can also work internationally, protecting calls made to offshore call centers. Source: http://www.scmagazineuk.com/development-of-call-protection-could-lead-to-the-end-of-the-theft-of-customer-payment-data-exchanged-over-the-telephone/article/172421/

Small banks are big problem in government bailout program. The Treasury Department's financial bailout has a growing problem on its hands, and this time, it has nothing to do with Wall Street. A new report from the agency shows that community banks continue to plague the program. A total of 101 bailed-out banks — nearly all are small — have missed paying the government a dividend, which was a condition of taking the aid. That number is up 25 percent since February, and has nearly doubled since November. The rising number of "deadbeat" banks, as they are known, could force Treasury to become more deeply entangled in the affairs of small financial firms that are troubled. The bailout legislation gives Treasury the right to appoint members to the boards of banks that miss six dividend payments. So far only one firm, Saigon National Bank in Southern California, has missed that many payments. Eight others have missed five payments and 16 have missed four. Most banks that received federal aid agreed to pay the government a 5 percent dividend every three months upon taking funds from the Troubled Assets Relief Program. Treasury officials declined to answer questions about whether they were preparing to make board appointments. Source: http://www.washingtonpost.com/wp-dyn/content/article/2010/06/13/AR2010061304513.html

Chemical and Hazardous Materials Sector

Stronger antiterror regulations urged for U.S. chemical sites. Chemical-security advocates are calling for Congress to pass stronger regulations on the types of chemicals used at U.S. facilities, pointing to the BP oil spill in the Gulf of Mexico as evidence of private companies' lack of preparation for a possible terrorist attack, Greenwire reported June 16. "The BP spill in the Gulf shows undeniably that worst-case scenarios can and do happen, and they can and do overwhelm any emergency response capacity," said a Center for American Progress consultant on high-risk chemical sites. "Oil in the water is really bad. Chemicals in a big city could be even worse." One chemical used by the oil industry to aid in the conversion of crude oil into gasoline is hydrofluoric acid. The acid is extremely poisonous for humans and has been judged by the U.S. Centers for Disease Control and Prevention to be a potential, chemical terrorism threat. The hydrofluoric acid housed at BP's Texas City site could endanger up to 550,000 residents if it were to be released, the oil firm acknowledged recently to the U.S. government. Source: http://www.globalsecuritynewswire.org/gsn/nw_20100617_6935.php

Commercial Facilities

(Arizona) **Bomb threat at Ronstadt Center.** Police are investigating a call of a bomb threat at the Ronstadt Center in downtown Tucson, Arizona. The Tucson Police Department said they received a call at 5:03 p.m. June 17 from a telephone number outside the area reporting that there was a bomb

at the center. Officers are searching the property for suspicious devices. Traffic is not being restricted at this time. Source: http://www.kgun9.com/Global/story.asp?S=12669616

(Idaho) **Bomb squad called to north Lewiston storage unit.** An improvised explosive device was found in North Lewiston, Idaho at the 7th Avenue North Mini Storage, June 17. The circular cylinder was detonated by Spokane County Bomb Disposal. Idaho State Police are investigating the case along with the Nez Perce County Sheriff's Office. They are not releasing the name of the owner of the storage unit or how they pinpointed the location. Source: http://www.klewtv.com/news/local/96620339.html

(California) **Explosion kills 1, injures 3 in Simi Valley.** An explosion has killed one person and injured three others at a business in a Simi Valley, California industrial area. Simi Valley firefighters responded to a police call at about 1:15 p.m. June 17. Businesses in a half-mile radius were evacuated. The blast appeared to have punched a hole through the building's roof. Three people have suffered minor injuries. A fourth person was later found dead at the scene. The cause of the blast is under investigation. Source: http://cbs2.com/local/Simi.Valley.Explosion.2.1758214.html

(New Mexico) **Socorro hotel probed for deadly disease.** The Best Western Inn in Socorro, New Mexico shut down its pool and spa after the state Health Department and the Environment Department said two people who stayed in the hotel contracted Legionnaire's disease. The health department said a test of the Best Western returned a positive sample for legionella, the bacteria that causes Legionnaire's disease. The Best Western owner said he has hired his own consultant who has tested the facility and said the results have come back negative, but he said he's not taking any chances. The spa and pool will go through an extensive cleaning process, but the hotel has remained open, the owner noted. The health department said it is nearing the end of its investigation, after contacting everyone who stayed in the hotel within two weeks of the people who contracted Legionnaire's disease. Source: http://www.koat.com/news/23901108/detail.html

(Michigan) **Man uses bomb threat during robbery.** The Oakland County Sheriff's Office said a man used a bomb threat to rob a gas station June 14 in Independence Township, Michigan. The office said the man walked into the Sunoco gas station and told the clerk he had a bomb in his pocket. The man got away with an undisclosed amount of cash and was last seen walking north away from the station. A K-9 unit was dispatched to the area following the robbery but couldn't locate the man. Source: http://www.clickondetroit.com/news/23907397/detail.html

(Florida) **Lehigh bomb threat used as robbery diversion, deputies say.** A man and woman called a bomb threat into a Lehigh Acres, Florida Walmart to distract authorities June 15 while they robbed a nearby pharmacy. Deputies were called to the Walmart off Lee Boulevard just before 5 p.m. in reference to a man who called the store and said there was a bomb in the food section. The store was evacuated as deputies searched the scene, but nothing harmful was found. While deputies were investigating the bomb scare, a man and woman were robbing Homestead Pharmacy off Homestead Road N. The victim said that at about 5 p.m., two people with weapons entered the store demanding Oxycodone and Xanax pills. After the victim gave them the pills, they ran from the store. Deputies arrived at the pharmacy and found the two suspects not far from the store. Detectives determined that they made the bomb threat as a diversion while they robbed the pharmacy. They have been charged with robbery with a weapon, and more charges are pending. Source: http://www.news-

press.com/article/20100615/CRIME/100615092/1075/Lehigh-bomb-threat-used-as-robbery-diversion--deputies-say

(New York) **Bomb threat forces evacuation of complex.** Police are still investigating a bomb threat at The Broad Street Complex in Horsheads, New York June 11. The complex houses several tenants including the YMCA Day Care Center, a senior citizens center and a gym. Authorities were able to get everyone out of the complex safely. No one was injured. Police said the evacuation took no more than an hour. Officials did not find any explosives in the building. The building is owned by the Horseheads School District. Police stated that they do not know who called in the threat. The chief stated that the building is now safe for community members to use again. Source: http://www.wetmtv.com/news/local/story/Bomb-Threat-Scare/vdd36E-epkWty__0-RR3eA.cspx

COMMUNICATIONS SECTOR

FCC eyes first step toward broadband regulation. The U.S. Federal Communications Commission (FCC) is scheduled to vote on the first step toward reclassifying broadband as a regulated, common-carrier service, despite objections from many U.S. lawmakers and broadband providers. The FCC was scheduled to vote June 17 on a notice of inquiry on new legal frameworks for enforcing network neutrality rules, redirecting telephone subsidies to broadband, and implementing other parts of the agency's national broadband plan. In a notice of inquiry, or NOI, the FCC seeks public comment on a topic. NOIs often lead to FCC rulemaking proceedings. The NOI follows a U.S. appeals court decision in April stating the FCC did not have the authority to enforce informal net neutrality rules in a case involving Comcast's throttling of some peer-to-peer traffic.The FCC Chairman has suggested that the appeals court ruling means the FCC has little authority to regulate broadband, and reclassifying broadband from a largely unregulated information service to a regulated common-carrier service would restore some of the agency's authority. Under the chairman's plan, the FCC would forbear from applying most of the common-carrier regulations under Title II of the Telecommunications Act to broadband. The main goals would be to create net neutrality rules prohibiting broadband providers from selectively blocking Web content, to reform the Universal Service Fund that now subsidizes telephone service in poor and rural areas, and to require broadband providers to give customers more information about the speeds and quality of service they receive, the chairman has said. Source: http://www.computerworld.com/s/article/9178144/FCC_eyes_first_step_toward_broadband_regulation

High-speed Internet rules might prove costly. Proposed regulation of high-speed Internet service providers by the U.S. government could cost the economy at least $62 billion annually over the next five years and eliminate 502,000 jobs, according to a study released by New York Law School. The report estimates that broadband providers and related industries may cut their investments by 10 percent to 30 percent from 2010 to 2015 in response to additional regulation. At 30 percent, the economy might sustain an $80-billion hit, according to the director of the law school's Advanced Communications Law & Policy Institute, which released the report June 16. "There will be follow-on effects in the whole ecosystem," said the president of technology researcher Entropy Economics in Zionsville, Ind., who co-authored the study with the director. "A diminution of investment by the big infrastructure companies will reduce network capacity, new services, and investment by all the ecosystem companies," such as application providers and device manufacturers, he said in an

interview. Source:
http://www.businessweek.com/technology/content/jun2010/tc20100616_751009.htm

Public safety agencies aim to stop spectrum auction. Ever since the September 11 attacks exposed the communications difficulty that police, fire and other personnel had in a crisis, government and public safety officials have wrestled with how to rebuild the nation's emergency networks. Nine years later, that effort has reached a showdown between the Federal Communications Commission, which is seeking to auction off a block of wireless broadband spectrum to the private sector, and public safety officials, who say that the additional space on the public airwaves should be used instead for a dedicated emergency broadband network. With commercial wireless companies preparing to build the next generation of wireless communication networks, the resolution of the debate will determine whether public safety officials will be able to use the latest technology in emergencies. The two sides will face off on June 17 at a hearing before the House Subcommittee on Communications, Technology and the Internet, which is considering legislation to pay for a public safety network. Source:
http://www.nytimes.com/2010/06/16/technology/16fcc.html

ATT has 3G data outage again. AT&T's 3G Data Network was down again June 11, and this time, Lafayette, Louisiana residents were not the only ones impacted. The failure affected customers across the southeastern United States, said an AT&T spokeswoman. Voice and text applications appeared to be working for most customers, but most could not send or receive multimedia messages or connect to the Internet. The spokeswoman said the company began receiving calls about the problem around 12:30 p.m. She said technicians had identified the cause of the outage as of 5 p.m. June 11 and were working to restore service. A similar outage occurred June 9 after a fiber-optic cable was cut in the Zachary area. The incident briefly disrupted data transfers in the Lafayette area. Source:
http://www.theadvertiser.com/article/20100612/BUSINESS/6120307

Solar flare activity might threaten GPS. A Cornell University expert on global positioning and satellite systems is warning they will be challenged as solar flare activity rises. A professor of electrical and computer engineering said an increasingly complex and brittle U.S. technical infrastructure has been created since 2004 — a period of minimum solar flare activity. And during future periods of solar activity, those systems will be tested for the first time. "We have been observing the sun during the space age for only 50 years and we do not fully understand its behavior, especially the extremes of its behavior," the professor said. "In 2006, there was an eruption of solar radiation 100 times more intense than expected that temporarily silenced many GPS receivers over the sun-lit Earth. What is the ultimate limit of such eruptions of solar energy? Is it 1,000 times more intense, 10,000 times more intense? We just don't know." Although the sun has been rather predictable during the past 50 or 60 years, it recently has become less predictable, the professor said, noting such activity calls into question man's understanding of how the sun operates and the ability to predict its impact on technology. "However, we do know that our increasingly more efficient infrastructure is also less robust and more vulnerable," he said. "Space weather — such as the upcoming period of increased solar activity — will test the vulnerabilities of our communications and navigation infrastructure." Source: http://www.gpsdaily.com/reports/Solar_flare_activity_might_threaten_GPS_999.html

DEFENSE INDUSTRIAL BASE SECTOR

(Maryland) **Md. man charged in plot to steal copper.** A federal grand jury has indicted an Annapolis, Maryland man on charges of theft in an alleged plot to steal copper cables worth more than $300,000. The indictment against the 54-year-old man was returned June 15. He was arrested June 17. According to the five-count indictment, he worked at AAI Corp. The federal government bought copper cables and other wire and stored the equipment at AAI. The indictment alleges that he took cables stored at AAI and sold them to a recycling center for cash. Source: http://wtop.com/?nid=25&sid=1983319

Vandenberg conducts test launch of Minuteman III missile. Vandenberg Air Force Base in Santa Barbara County, California announced Wednesday that it had conducted a successful test launch of an unarmed Minuteman III Intercontinental Ballistic Missile. Traveling 4,190 miles across the Pacific Ocean to a target in the Kwajalein Atoll in the Marshall Islands, the missile was made up of parts from the Department of Defense's three nuclear missile bases — F.E. Warren Air Force Base in Wyoming, Minot Air Force Base in North Dakota and Malmstrom Air Force Base in Montanta. The test was conducted by the Vandenberg-based 576th Flight Test Squadron, which although it had been under the command of Vandenberg's 30th Space Wing, is now part of the Air Force Global Strike Command. Source: http://nosint.blogspot.com/2010/06/vandenberg-conducts-test-launch-of.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+blogspot/fqzx+(Naval+Open+Source+INTelligence)

F-35B STOVL fighter goes supersonic. The short-takeoff and vertical-landing version of the F-35 Joint Strike Fighter flew past the sound barrier June 10, becoming the first U.S. STOVL aircraft to exceed that milestone. A Marine Corps pilot flew the F-35B test aircraft, known as BF-2, to a speed of Mach 1.07, or 727 miles-pe- hour. The test run took place at an altitude of 30,000 feet over an off-shore supersonic test track near Naval Air Station Patuxent River, Md. The achievement came on the aircraft's 30th test flight. Aircraft manufacturer Lockheed Martin reported that the pilot accomplished 21 unique test points during the flight, including validation of roll, pitch, yaw and propulsion performance. Further testing, according to Lockheed, will gradually expand the flight envelope out to the aircraft's top speed of Mach 1.6 — a speed the aircraft is designed to reach while carrying a full internal weapons load of more than 3,000 pounds. Customers for the F-35B include the Marine Corps and the British Royal Navy. The aircraft is to be the first JSF version to become operational, and is scheduled to enter service with the Marines in late 2012. Two F-35A conventional takeoff-and-landing test aircraft produced for the Air Force also have broken the sound barrier. A carrier-capable version of the JSF, the F-35C, is being produced for the Navy. Source: http://www.militarytimes.com/news/2010/06/dn_jsf_supersonic_061410/

(California) **Big new Navy ship ready for sea trials.** The USNS Charles Drew — the new 684-foot dry cargo ship that bears the name of the pioneering surgeon who created large, life-saving blood banks during World War II — will achieve a milestone early Wednesday when the vessel leaves the NASSCO/General Dynamics yard for its first extensive sea trials. Workers are scheduled to remove the $500-million ship's mooring lines at 7:45 a.m., enabling the Charles Drew to sail out of San Diego Harbor for weeks of rigorous testing far offshore, the company said. The ship is one of the last Lewis

and Clark-class cargo ships that NASSCO is scheduled to build for the Navy. Source: http://www.signonsandiego.com/news/2010/jun/15/grsq-huge-nassco-ship-ready-sea-trials/

Critical Manufacturing

Suzuki recalls Grand Vitara, XL-7. Suzuki is recalling about 47,000 Grand Vitaras from the 2006 model year and XL-7s from the 2005-2006 model years because of a problem with the power assist pump. The company said the tension adjuster pulley on the pump's drive belt could break, causing the drive belt to come off, and disabling the power steering. Dealers will repair the problem at no charge. Owners may contact Suzuki at 1-800-934-0934 about Recall No. SB. Source: http://www.consumeraffairs.com/recalls04/2010/suzuki_vitara.html

BMW recalls 2008-2011 1-series models. BMW is recalling certain 2008-2011 BMW 1-series vehicles. The company said that the seat belt pre-tensioner insulation could ignite. The company has not yet provided a remedy or an owner-notification schedule. Owners may contact BMW at 1-800-525-7417. Source: http://www.consumeraffairs.com/recalls04/2010/bmw1.html

Volkswagen recalls 2009 Routan. Volkswagen is recalling about 16,000 2009 Routans. The company said the wiring harness may be defective, which could lead to a short circuit and, possibly, a fire in the sliding side door. Dealers will inspect the wiring and, if necessary, make repairs. Owners may contact Volkswagen at 1-800-822-8987 about Recall No. 9758/T7. Source: http://www.consumeraffairs.com/recalls04/2010/vw_routan.html

Boeing 747-8 freighter receives expanded type inspection authorization. Boeing received expanded type inspection authorization (TIA) from the U.S. Federal Aviation Administration (FAA) for the 747-8 Freighter June 11. This authorization clears the way for FAA personnel to participate in test flights and collect required data. With the issuance of TIA, the 747 program is beginning expanded certification testing. During this phase of testing, the extremes of the flight envelope are explored. Testing conditions include operations in hot and cold weather as well as takeoffs and landings at high-altitude airports. In addition, over-speed conditions, hard landings and engine-out conditions are tested. The entire flight-test program calls for a total of about 3,700 hours of ground and air testing. The first 747-8 Freighter delivery is planned for the fourth quarter of this year. The first customer is Cargolux. Source: http://blog.seattlepi.com/worldairlinenews/archives/211153.asp

Emergency Services

Standards announced for private sector preparedness. The Department of Homeland Security (DHS) announcement of adoption of standards for the Voluntary Private Sector Preparedness Accreditation and Certification (PS-Prep) program marks a major milestone. Under an agreement with DHS, the ANSI-ASQ National Accreditation Board will be the accreditation body for the PS-Prep Program. Accreditation will be offered under the ANSI-ASQ National Accreditation Board's ANAB brand. "Private organizations across the country — from businesses to universities to non-profit organizations — have a vital role to play in bolstering our disaster preparedness and response capabilities," the DHS Secretary said. "These new standards will provide our private sector partners with the tools they need to enhance the readiness and resiliency of our nation." The adoption of the standards — developed by the National Fire Protection Association, the British Standards Institution,

and ASIS International — was published in a June 16, 2010, Federal Register notice following a series of regional public meetings and the incorporation of public comments. Source: http://www.wisbusiness.com/index.iml?Article=200246

Department of Homeland Security awarded over $11.9 million for fire station construction grants. The Department of Homeland Security (DHS) awarded more than $11.9 million in American Recovery and Reinvestment Act (ARRA) funds for Fire Station Construction Grants, the DHS Secretary announced Friday. The funds will be used to support U.S. first responders while creating jobs and stimulating local economies. The funds were awarded to three grants selected hrough a competitive review process on existing fire stations. The current unsafe or uninhabitable structures will be replaced or modified in order to enhance response capabilities and protect communities from fire-related hazards. The fire protection coverage should be in compliance with National Fire Protection Association standards Source: http://wireupdate.com/wires/6358/department-of-homeland-security-awarded-over-11-9-million-for-fire-station-construction-grants/

(Michigan) **911 outage highlights need for back-up plans.** Emergency officials from across central and lower Michigan will meet next week to discuss why 911 service went dark for several hours on Wednesday and into Thursday and what can be done to prevent it. “This just showed us how important this is - we have a fault,” said the emergency management program manager with the Ingham County Sheriff’s Office. The 911 service went down Wednesday about 7 p.m. Calls were disrupted to varying degrees in portions of at least seven counties and weren’t restored in some areas such as East Lansing until 4 a.m. the following day. Service went down after a telephone line was cut by a third party that happened to be digging. There were unconfirmed reports to AT&T that the line was cut by a farmer tilling in the Lowell area in Kent County, and at the height of the problem, the outage stretched from Ottawa County across Greater Lansing and down to Hillsdale County. There have been no reports of serious calls that were missed but “we were all sweating what’s going to happen,” the emergency management official said. Emergency 911 centers relied on social media such as Twitter and Facebook and on traditional newspaper and television Web sites to remind residents to call the 10-digit non-emergency number if they needed help. Source: http://www.lansingstatejournal.com/article/20100612/NEWS01/6120319/1002/NEWS01

Energy

Money trumps security in smart-meter rollouts, experts say. In a rush to take advantage of U.S. stimulus money, utilities are quickly deploying thousands of smart meters to homes each day — smart meters that experts say could easily be hacked. The security weaknesses could potentially allow miscreants to snoop on customers and steal data, cut off power to buildings, and even cause widespread outages, according to a number of experts who have studied the meters, and looked into smart-grid systems. A new paper out of the University of Cambridge highlights privacy concerns from smart meters, as well as security risks caused by linking home-area networks, of which smart meters are an initial piece, to utilities. “From a hardware perspective, cell phones today are more secure than many of the smart meters in deployment,” said a security researcher based in Germany who has previously analyzed mobile phone and smart-card security. “Those meters, however, may be used as attack vectors into the spheres of power distribution and generation, as well as into customer

databases at the utilities," the security researcher said. Source: http://news.cnet.com/8301-27080_3-20007672-245.html

(Connecticut) **Copper thieves are stealing power lines.** Copper crooks have stolen power lines 17 times since November from United Illuminating Co. (UI) in Bridgeport, Easton, Fairfield, Orange and other Connecticut towns. The thefts total about 6,000 feet of cable, and the most recent incident was last week. Copper thefts have been on the increase throughout the country recently, as the commodity's price has risen from $1.29 per pound in early 2009 to a recent high of $3.79, before settling back to just above $3 per pound. The rash of copper thefts was a first for UI, a spokesman for the the southern Connecticut power company said — even though copper briefly climbed above $4 per pound a few years ago. Connecticut Light & Power has seen an increase in attempted thefts lately, a company spokesman said. Most recently, thieves removed $60,000 worth of copper from a substation in Hartford, and were caught when they tried to sell it because scrap dealers alerted police. "The incidents have pretty much reflected the price of copper," he said. "When the price goes up, incidents of theft go up, when it goes down, thefts go down." Source: http://www.courant.com/business/hc-copper-theft-0616-20100616,0,1268056.story

House approves GRID Act. The President would gain new powers over the U.S. electrical grid under a bill the House of Representatives approved June 9. The Grid Reliability and Infrastructure Defense Act would permit the President to order immediate emergency measures to protect the reliability of the bulk-power system or defend critical electric infrastructure against an imminent grid security threat. The GRID Act passed the House on voice vote; it now lies before the Senate Energy and Natural Resources Committee. The bill would also have the Federal Energy Regulation Commission issue a rule within 180 days requiring high-voltage electric transmission companies to address the so-called Aurora vulnerability. In 2006, the Homeland Security Department staged a test dubbed "Aurora" at the Idaho Energy Laboratory that demonstrated that an attacker could hack into the control system of an electric generator, causing severe physical damage to the equipment. The bill's accompanying report complains that the North American Electric Reliability Corporation, the bulk power industry's self-regulatory organization, has been slow to react to grid security concerns. NERC has yet to propose a reliability standard to address an Aurora vulnerability and NERC critical infrastructure protection standards apply only to owners and operators who self-identify their assets as critical, the report adds. Source: http://www.fiercegovernmentit.com/story/house-approves-grid-act/2010-06-13

Food and Agriculture

Iowa firm recalls frozen chicken products due to possible salmonella contamination. ConAgra Foods Packaged Foods is recalling Marie Callender's brand Cheesy Chicken and Rice frozen meals, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced June 17. The product subject to recall include: 13-ounce packages of "Marie Callender's Cheesy Chicken & Rice White Meat Chicken and Broccoli over Rice Topped with Rich Cheddar Sauce." The company is recalling all meals in commerce, regardless of production date. These products are being recalled after the company was informed by the U.S. Centers for Disease Control and Prevention (CDC) of an investigation involving 29 people in 14 states who have been diagnosed with salmonellosis linked to Salmonella serotype Chester. Eight of the patients specifically reported eating this product in April and May 2010, prior to illness onset; the last reported illness was reported May 22. FSIS became aware of the problem during the course of an ongoing investigation of a multi-state outbreak of

Salmonella serotype Chester illnesses. CDC, the Food and Drug Administration (FDA), FSIS, and state health and agriculture departments are cooperating in this ongoing investigation. Source: http://www.fsis.usda.gov/News_&_Events/Recall_036_2010_Release/index.asp

Texas firm recalls three varieties of 'SpaghettiOs'. Campbell Soup Supply Company is recalling approximately 15 million pounds of "SpaghettiOs with Meatballs" canned products due to possible under-processing, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced June 17. The following products are subject to recall: 14.75-ounce cans of "SpaghettiOs" with Meatballs, bearing the identifying product code "U5" on the bottom of the can; 14.75-ounce cans of "SpaghettiOs" A to Z with Meatballs, bearing the identifying product code "4N" on the bottom of the can; 14.75-ounce cans of "SpaghettiOs" Fun Shapes with Meatballs (Cars), bearing the identifying product code "KS" on the bottom of the can. The problem was discovered through a routine warehouse inspection by the company and its subsequent investigation. FSIS has received no reports of illnesses from consumption of these products. Source: http://www.fsis.usda.gov/News_&_Events/Recall_035_2010_Release/index.asp

Regulators consider broadening testing for E. coli. The food industry and government regulators have focused for years on finding the most virulent strain of E. coli bacteria, which every year sickens thousands. But they don't regularly test for six less common E. coli strains that can cause illnesses equally as serious. Industry officials said tests aren't available to do widespread monitoring of these other strains, but food-safety advocates have begun pushing the government to step up surveillance after several outbreaks. The food industry screens for the most prevalent strain, O157:H7, which belongs to a class of E. coli that produces a sickening toxin and causes an estimated 73,000 illnesses each year. Symptoms include bloody diarrhea, dehydration and, in severe cases, kidney failure. It is the only strain the U.S. Department of Agriculture considers an adulterant in meat, requiring regular screening and recalls. Six other E. coli strains that also produce the toxin account for the majority of of non-O157 E. coli cases — estimated at 30,000 illnesses in the U.S. each year, according to the Centers for Disease Control and Prevention. But just 5 percent of public health laboratories nationally test for these strains, so there is no reliable way to know whether the number of illnesses is increasing. Source: http://www.google.com/hostednews/ap/article/ALeqM5jZz8LSjhfQyF2h96n6BHdcw12iIAD9GCE8A01

Lobster meat recall. Portland Shellfish Company, Inc. of Portland, Maine is voluntarily recalling the following brands of cooked, ready to eat fresh or frozen lobster meat: Portland Shellfish Co. Inc brand, Claw island, Craig's All Natural, and Inland Ocean cooked, fresh or frozen lobster claw and knuckle meat. Recent tests show the product has the potential to be contaminated with Listeria monocytogenes, an organism which can cause serious and sometimes fatal infections. Source: http://www.wusa9.com/news/local/story.aspx?storyid=102542&catid=28

Kroger announces ice cream recall. The Kroger Co. is recalling select containers of Kroger Deluxe Chocolate Paradise Ice Cream sold in 17 states because it may contain tree nuts not listed on the label. Customers should return the product to stores for a full refund or replacement. People who are allergic to tree nuts could have a serious or life-threatening reaction if they consume this product. For consumers who are not allergic to tree nuts, there is no safety issue with the product. The product was sold in Kroger stores in Alabama, Arkansas, Georgia, Illinois, Indiana, Kentucky, Louisiana, Michigan, Mississippi, Missouri, North Carolina, Ohio, South Carolina, Tennessee, Texas, Virginia, and

West Virginia. The recall also includes Jay C, Food 4 Less, Hilander, Owen's, Pay Less, and Scott's stores in Illinois and Indiana. Other stores Kroger operates under different banner names are not included in this recall. The Kroger Deluxe Chocolate Paradise Ice Cream is sold in 48-ounce containers with a "sell by" date of Jan. 24, 2011, under the following UPC code, 11110 50712. This is the only sell-by date affected by this recall. Kroger is using its Customer Recall Notification system that alerts customers who may have purchased recalled Class 1 products through register receipt tape messages and phone calls. Source: http://www.newsplex.com/home/headlines/96303519.html

FDA cautions on accurate vitamin D supplementation for infants. The Food and Drug Administration alerted parents and caregivers June 15 that some liquid Vitamin D supplement products are sold with droppers that could allow excessive dosing of Vitamin D to infants. The FDA also advised manufacturers of liquid Vitamin D supplements that droppers accompanying these products should be clearly and accurately marked for 400 international units (IU). In addition, for products intended for infants, FDA recommends that the dropper hold no more than 400 IU. The American Academy of Pediatrics (AAP) has recommended a dose of 400 IU of Vitamin D supplement per day to breast-fed and partially breast-fed infants. The easiest way to ensure that an infant will not get more than the recommended dose is to use a product supplied with a dropper that will give no more than 400 IU per dose. Excessive amounts of Vitamin D can be harmful to infants, and may be characterized by nausea and vomiting, loss of appetite, excessive thirst, frequent urination, constipation, abdominal pain, muscle weakness, muscle and joint aches, confusion, and fatigue, as well as more serious consequences such as kidney damage. Source: http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm215150.htm

NOAA, FDA continue ramping up efforts to ensure safety of Gulf of Mexico seafood. The National Oceanic and Atmospheric Administration (NOAA) and the U.S. Food and Drug Administration (FDA) are taking additional steps to enhance inspection measures designed to ensure that seafood from the Gulf of Mexico reaching America's tables is safe to eat. The federal government, in conjunction with Gulf States' regulatory agencies, is playing an active role in ensuring the safety of seafood harvested from federal and state waters. The government is taking a multi-pronged approach to ensure that seafood from Gulf waters is not contaminated by oil. The strategy includes precautionary closures, increased seafood-testing inspections and a re-opening protocol. The federal effort will also include NOAA's dockside sampling of fish products in the Gulf. NOAA will verify that catch was caught outside the closed area using information from vessel-monitoring systems that track the location of a vessel or information from on-board observers. FDA will first target oysters, crab, and shrimp, which due to their biology retain contaminants longer than finfish, for additional sampling. The sample collection will target primarily seafood processors who buy seafood directly from the harvester. Source: http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm215493.htm

(Illinois) **State counts 79 salmonella cases linked to Subway.** The number of Salmonella cases connected to Illinois Subway restaurants continues to grow. The Illinois Department of Public Health said there are now 79 confirmed cases of the rare Salmonella serotype Hvittingfoss, with the age range of the people who have been sickened after eating at a Subway ranging from 2 to 79. Cases have been reported in connection with Subway restaurants in 26 counties: Bureau, Cass, Champaign, Christian, Coles, DeKalb, DeWitt, Fulton, Henry, Knox, LaSalle, Livingston, Macon, Marshall, McLean, Moultrie, Ogle, Peoria, Sangamon, Schuyler, Shelby, Tazewell, Vermilion, Warren, Will and Winnebago. All illnesses started between May 14 and May 25. Health officials said their investigation

is ongoing. Following the initial outbreak, Subway voluntarily withdrew all lettuce, green peppers, red onions and tomatoes from the suspected dates and replaced them with new, fresh produce, according to the state public health department. Source: http://www.news-gazette.com/news/politics-and-government/2010-06-15/state-counts-79-salmonella-cases-linked-subway.html

Lax food safety in restaurants, researcher finds. A review of restaurant food safety practices found that a typical kitchen worker cross-contaminates food with potentially dangerous pathogens about once per hour. Among the risky behaviors cited were workers using aprons and other garments to dry hands, as well as using the same utensils and surfaces to prepare both raw and cooked foods, according to a review by a North Carolina State University researcher. Both practices are considered health violations, said an assistant professor and food safety specialist who used video cameras in eight restaurant kitchens to monitor worker food-safety habits. A food policy representative for the National Restaurant Association said that while the study is disconcerting, the association doesn't feel it is representative of the entire restaurant industry. Source: http://www.msnbc.msn.com/id/37646777/ns/health-food_safety/

Government Sector (including Schools and Universities)

(California) **Police find no explosive in box outside NoHo H.S.** Los Angeles police say no explosives were found in a box that was left in front of North Hollywood High School. The box found outside the school's front doors early Thursday had wires hanging out. An officer said police determined that the box was harmless after a robotic device was used to investigate it. Police and Los Angeles Unified School District representatives said a custodian discovered the box shortly after 6 a.m. Dozens of arriving students were kept on bleachers at a football field while the robot worked. A district spokeswoman said the school did not receive any bomb threats. She said the campus will hold graduation ceremonies in the evening, but there will be additional security. Source: http://cbs2.com/local/suspicious.package.North.2.1757114.html

2 charged in Mass. with conspiring to aid Al Qaeda. Two men accused in a terror plot to kill Americans face new federal charges that they conspired to provide personnel, advice, assistance and other services to Al Qaeda. A grand jury Thursday added charges of conspiring to provide material support to a designated foreign terrorist organization in a superseding indictment against a 27-year-old suspect from Sudbury, Massachusetts, and a 28-year-old suspect. Authorities said the 28-year-old suspect, who used to live in Mansfield, Massachusetts, is now in Syria. The men face up to 15 years in prison and a fine of $250,000 if convicted of the latest charge. When reached by phone, the first suspect's lawyer did not comment. The suspects already face a 10-count indictment. Prosecutors said the men conspired to kill American troops in Iraq, assassinate two unnamed U.S. politicians, and shoot shoppers in U.S. malls.Source: http://www.foxnews.com/us/2010/06/17/charged-mass-conspiring-aid-al-qaeda/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+foxnews/us+(Text+-+US)

Alert issued for 17 Afghan military members AWOL from U.S. air force base. A nationwide alert has been issued for 17 members of the Afghan military who have gone AWOL from an Air Force base in

Texas where foreign military officers who are training to become pilots are taught English, FoxNews.com has learned. The Afghan officers and enlisted men have security badges that give them access to secure U.S. defense installations, according to the lookout bulletin, "Afghan Military Deserters in CONUS [Continental U.S.]," written by Naval Criminal Investigative Service in Dallas and obtained by FoxNews.com. The Be-On-the-Lookout (BOLO) bulletin was distributed to local and federal law enforcement officials Wednesday night. The Afghans were attending the Defense Language Institute (DLI) at Lackland Air Force Base in Texas. The DLI program teaches English to military pilot candidates and other Air Force prospects from foreign countries allied with the U.S. "I can confirm that 17 have gone missing from the Defense Language Institute," said the chief of public affairs, 37th Training Wing, at Lackland AFB. "They disappeared over the course of the last two years, and none in the last three months." Source: http://www.foxnews.com/us/2010/06/17/afghan-military-deserters-missing-air-force-base/

(California) **Teen arrested after bomb explodes at Menlo Park school field.** A 17-year-old boy was arrested late Wednesday night on suspicion of detonating an explosive device near La Entrada Middle School in Menlo Park, California police said. Neighbors called police to report hearing a loud explosion in the Sharon Heights neighborhood at about 10:10 p.m. The teenager was found near the middle school soon after the explosion, and he admitted to detonating a homemade bomb in the grass field directly behind the school, police said. A spokeswoman for the Menlo Park Police Department said the device was possibly a pipe bomb. "The juvenile said he got the materials from a local hardware store," the spokeswoman said. No injuries or substantial property damage were reported, according to police. The teenager was arrested on suspicion of possessing and detonating an explosive device and cited before being released to his parents, the spokesman said. She described the teenager as cooperative. "He led investigators to believe that he wasn't trying to cause harm to anybody or any property," she said. "That's why he chose that particular time and place to do it." Source: http://www.mercurynews.com/breaking-news/ci_15322232?nclick_check=1

Cybersecurity: Continued attention Is needed to protect federal information systems from evolving threats. Pervasive and sustained cyber attacks continue to pose a potentially devastating threat to the systems and operations of the federal government. In recent testimony, the Director of National Intelligence highlighted that many nation states, terrorist networks, and organized criminal groups have the capability to target elements of the United States information infrastructure for intelligence collection, intellectual property theft, or disruption. In July 2009, press accounts reported attacks on Web sites operated by major government agencies. The ever-increasing dependence of federal agencies on information systems to carry out essential, everyday operations can make them vulnerable to an array of cyber-based risks. Thus it is increasingly important that the federal government carry out a concerted effort to safeguard its systems and the information they contain. GAO is providing a statement describing (1) cyber threats to federal information systems and cyber-based critical infrastructures, (2) control deficiencies that make federal systems vulnerable to those threats, and (3) opportunities that exist for improving federal cybersecurity. In preparing this statement, GAO relied on its previously published work in this area. Source: http://www.gao.gov/products/GAO-10-834T

(Virginia) **Fake IDs could be helping thieves gain access to government offices in Arlington.** Arlington County police and federal authorities are investigating a series of recent thefts from office buildings that they think have been carried out by people who have been posing as legitimate workers with

fake identity badges. Authorities said they think the suspect or suspects have been hanging around entrances to office buildings, including those that house government offices, and have been gaining entry by following workers inside or being allowed in. Law enforcement officials said it appears the thefts target personal possessions — such as wallets, purses, credit cards and cash — belonging to those who work in the offices. Law enforcement agencies urged people to use caution when allowing anyone into secure buildings and to always ensure that people wearing badges scan themselves in. Arlington police said they are looking into the cases along with the U.S. Secret Service. A spokesman for the Secret Service declined to comment because of the ongoing investigation. Source: http://www.washingtonpost.com/wp-dyn/content/article/2010/06/15/AR2010061505326.html

New cyber security threats facing the public sector. The U.S. government is investing heavily in cyber security after the recent attacks on Google pushed the issue of targeted Internet security breaches up the agenda. Security experts said the attacks represent a new kind of security assault that can overcome the defenses of even sophisticated companies such as Google. They are carried out by "motivated" and organized people, and are targeted at a specific organization, according to the head of enterprise security services at Detica, who spoke at the recent conference on Modernizing Justice Through IT. The types of attacks Google experienced may be infrequent, but the Detica head predicts they will likely increase as Internet use grows, and business systems increasingly rely on cloud computing. Some attacks might stem from the stereotypical "casual attacker" - a teenager in his bedroom - but cyber attacks are also increasingly becoming a way for hostile foreign states to attack other countries as the technology gets more sophisticated. He said more people will get the skills needed to launch assaults on the systems of any organization with the aim of getting hold of data, causing operational problems, or making a political point. Source: http://www.computerweekly.com/Articles/2010/06/17/241633/New-cyber-security-threats-facing-the-public-sector.htm

(Michigan) **Bomb threats made, several county buildings temporarily closed.** Three county buildings in downtown Mount Clemens, Michigan have been reopened after they were shut down this morning due to a suspect repeatedly calling in bomb threats. According to a spokesman with the Macomb County Sheriff's Office, a suspect placed a call to the Macomb County Prosecutor's Office just after 9 a.m. the morning of June 15, stating that there was a bomb located at the sheriff's office. Shortly after, a second call was made to the same location and this time, the suspect said that a bomb would detonate at the sheriff'soOffice at 10: 30 a.m. A third, undecipherable phone call was made and then a fourth call, a hang up, occurred. A fifth call was made to the 41-A District Court in Sterling Heights. "Our 41-A District Court got a phone call probably around 10:30 (a.m.)," said a lieutenant with the Sterling Heights Police Department. "It was a bomb threat, but it wasn't for 41-A — it was for Circuit Court in Mount Clemens." Due to safety concerns, employees and the public inside three county buildings in downtown Mount Clemens were evacuated, including Macomb County Circuit Court. The spokesman said that the evacuation, which involved more than 1,000 people, went smoothly. Source: http://www.candgnews.com/Homepage-Articles/2010/06-09-2010/Bomb-threats-closings.asp

(Florida) **MacDill AFB open as usual a day after armed couple's arrest.** One day after a heavily armed couple tried to enter MacDill Air Force Base – where the Iraq and Afghanistan wars are coordinated – traffic is moving smoothly through all gates, said a base spokesman. A man and a woman are in custody after officials said they tried to enter the base's Bayshore Boulevard gate about 5 p.m. Monday in a sport utility vehicle carrying weapons and military gear, MacDill officials

said. Base officials haven't heard that it was a planned attack, and authorities did not find any explosives. A News Channel 8 reporter on scene at the base Monday night saw at least 13 loaded rifle magazines and two pistol magazines in a bag. Authorities also found military clothing and other military-style equipment in the grayish blue Honda CRV driven by the suspects. The suspects, who haven't been identified, didn't have proper identification cards to get on the base as a civilian or as a member of the military, officials said. Authorities haven't said if they tried to use fake IDs. Source: http://www2.tbo.com/content/2010/jun/15/macdill-afb-open-usual-day-after-armed-couples-arr/news-breaking/

(Maine) **Bomb threat found at Sea Road School.** Sea Road School in Kennebunk, Maine was evacuated for more than an hour and a half June 11 after a bomb threat was found in a bathroom at the school. A fifth-grade student found a note that read "I have a bomb" written on the girls' bathroom stall near the toilet paper dispenser around 9:30 a.m. The building was evacuated, and students were bused to the Kennebunk Elementary School. More than half a dozen officers went through the school and determined that it was safe for students to return just before 11 a.m. The Kennebunk Police Department has no leads at this time but said that the investigation will continue. This was the third bomb threat in a district school in three weeks.Source: http://www.seacoastonline.com/apps/pbcs.dll/article?AID=/20100611/NEWS/100619964/-1/NEWSMAP

(Minnesota; District of Columbia) **Hacker charged with threatening US VP using neighbor's PC.** A hacker tried to frame his neighbor by tapping into his Wi-Fi and sending threatening e-mails to the U.S. Vice President, according to FBI search warrant affidavits unsealed last week. A 45-year-old computer expert from Blaine, Minnesota is charged with using someone else's computer to send a threatening e-mail to the Vice President. However, the affidavits reveal years of disputes between him and neighbors from different areas where he has lived. The threat to the Vice President read, in part: "This is a terrorist threat! Take this seriously. I hate the way you people are spending money you don't have ... I'm assigning myself to be judge, jury and executioner. Since you folks have spent what you don't have, it's time to pay the ultimate price." According to the FBI, the suspect had also been using his technical skills to harass his current neighbors, and was alleged to have sent indecent images of children to his neighbor's work colleagues, using fake e-mail accounts he'd set up in the neighbors' name. He is also alleged to have stolen personal information and sent offensive messages. The suspect was charged with one count of aggravated identity theft and one count of threats to the President and successors to the presidency. He is scheduled to appear in federal court this week. Source: http://www.theregister.co.uk/2010/06/14/ardolf_charged/

Information Technology and Telecommunications

Google Wi-Fi data grab snared passwords, e-mail. Wi-Fi traffic intercepted by Google's Street View cars included passwords and e-mail, according to the French National Commission on Computing and Liberty (CNIL). CNIL launched an investigation last month into Google's recording of traffic carried over unencrypted Wi-Fi networks, and has begun examining the data Google handed over as part of that investigation. Google revealed May 14 that the fleet of vehicles it operates to compile panoramic images of city streets for its Google Maps site had inadvertently recorded traffic from unencrypted Wi-Fi networks. Google's intention was only to record the identity and position of Wi-Fi hotspots in order to power a location service it operates, the company said. However, the software it used to

record that information went much further, intercepting and storing data packets too. At the time, Google said it only collected "fragments" of personal Web traffic as it passed by, because its Wi-Fi equipment automatically changes channels five times a second. However, with Wi-Fi networks operating at up to 54M bits per second, it always seemed likely that those one-fifth of a second recordings would contain more than just "fragments" of personal data. That has now been confirmed by CNIL, which since June 4 has been examining Wi-Fi traffic and other data provided by Google on two hard disks, and over a secure data connection to its servers. Data-protection authorities in Spain and Germany have also asked Google for access to Wi-Fi traffic data intercepted in their countries, but the CNIL was the first to have its request granted, it said. Source: http://www.computerworld.com/s/article/9178220/Google_Wi_Fi_data_grab_snared_passwords_e_mail_

3.7 billion phishing emails were sent in the last 12 months. Cybercriminals sent 3.7 billion phishing emails over the last year, in a bid to steal money from unsuspecting web users, says CPP. Research by the life assistance company revealed that 55 percent of phishing scams are fake bank emails, which try and dupe web users into giving hackers their credit card number and online banking passwords. Hoax lottery and competition prize draws and 'Nigerian 419' scams that involve email requests for money from supposedly rich individuals in countries such as Nigeria, were also among the most popular phishing emails. Furthermore a quarter of Brits admitted to falling for the scams, losing on average 285 pounds. Online banking fraud has surged by 132 percent during the last year. The report also highlighted that 46 percent of web users worry their credit card details will be used to make illegal online purchases. CPP also revealed social networking scams are on the rise. Nearly one fifth of Brits have received phoney Facebook messages claiming to be from friends or family in the past year. One in 10 fear that fraudsters are using Twitter to follow them, while a third are concerned their social networking account could be hacked. Source: http://www.networkworld.com/news/2010/061610-37-billion-phishing-emails-were.html?hpg1=bn

Remote working poses threat to corporate security. A recent survey of 200 UK IT directors has found that 92 percent believe that, by allowing more staff to work remotely, they are increasing their security risks. Even though all respondents said that their workforce was increasingly mobile, 80 percent admitted they found it difficult to manage and secure ever-more sophisticated mobile devices. A researcher from Aruba Networks comments: "As smart phones and other mobile devices become increasingly popular, they pose an increasing security threat to the unprepared business. For an easier life, many IT departments would choose to limit the devices that are allowed to access corporate networks – but with demand for the coolest gadgets often coming from senior executives – this choice is often taken away from them." As demonstrated by the survey, today's challenge is how to support such a wide variety of devices, particularly as most of these devices were not built with business needs in mind. Source: http://www.net-security.org/secworld.php?id=9413

Mass website hack aimed at online gamers. According to the latest analysis, the mass Web site hacks which have been showing up over the last week are aimed at stealing access credentials for online games. The hackers' most prominent victims serving the malware have been the Wall Street Journal and the Jerusalem Post Web sites. The hacked Web servers are all Microsoft Internet Information Server (IIS) and ASP-NET-based, but analysis by a number of security services providers has shown that the attacker has used SQL injection vulnerabilities in custom Web applications to hack the sites. Administrators are advised to check their systems for any signs of interference and tampering. The

SQL injection vulnerability allows attackers to write their own HTML and JavaScript to the hacked sites content-management system's database. Specifically, the attackers embedded code which uploads an exploit for the recently discovered vulnerability in Flash Player into an iFrame. The code then tries to infect the hacked sites visitors' systems with trojans. It appears the attackers objective is to steal access data to Asian gaming Websites such as aion.plaync.co.kr, aion.plaync.jp and df.nexon.com. The Flash Player vulnerability has been fixed in version 10.1. A Chinese group known as dnf666, which was also responsible for a major SQL injection attack in March, appears to be behind the attack. Source: http://www.h-online.com/security/news/item/Mass-website-hack-aimed-at-online-gamers-1022506.html

Senators unveil long-awaited cybersecurity bill. The long-awaited cybersecurity and Federal Information Security Management Act (FISMA) reform bill introduced June 10 by the leaders of the Senate Homeland Security and Governmental Affairs Committee would create two cybersecurity directors - one in the White House and the other in the Department of Homeland Security - to lead the federal government's information security efforts. The Protecting Cyberspace as a National Asset Act of 2010 also would provide a framework for the president to authorize emergency measures to protect the mostly privately owned critical IT infrastructure - such as financial networks and utility grids - if a cyber attack is imminent. Owners of these critical IT systems could face civil penalties if they do not follow regulations to secure them properly. The bill provides for the government and industry to collaborate on defining regulations and situations when a cyber emergency could be declared. The bill also would reform FISMA, the 8-year-old law that governs how federal agencies secure their IT systems by jettisoning the paper-based compliance process with one that emphasizes continuous monitoring of computer systems and red-team assaults by "friendly hackers" to test vulnerabilities. Source: http://www.bankinfosecurity.com/articles.php?art_id=2631

New wave of website hacks seek to spread malware. Those behind the SQL injection attack that compromised pages belonging to the Wall Street Journal and a number of other sites are at it again, according to researches at malware detection solutions provider Sucuri Security. The latest wave of attacks began June 11 and, at that time, 1,000 pages, including the Web sites for Chicago Public Radio and IndustryWeek, were infected, the lead security researcher at Sucuri Security, told SCMagazineUS.com June 11. The sites were injected with JavaScript code that attempted to load malware from a new malicious Web server onto visitors' PCs, researchers said. As of June 11, the server was still active. "They [attackers] just started using a different site to host the malware, which is still live, so these sites are currently actively serving malware to their users," the lead security researcher said. Some of the same sites that were infected earlier this week were reinfected in the latest attack, he added. Since the second round of the attack just began, it is difficult to determine the extent, so the actual number of infected sites might be greater than 1,000. Ironically, one of the infected sites was Idera.com, a provider of SQL Server and SharePoint administration tools. Just like the last wave of attacks, all affected sites are hosted on Microsoft Internet Information Services (IIS) web servers, and using Active Server Pages software from ASP.net. Source: http://www.scmagazineus.com/new-wave-of-website-hacks-seek-to-spread-malware/article/172213/

Taliban hacked, DoD starts cyber offensive. The Webmaster of a Taliban-endorsed Webs ite has claimed that the site was hacked. An administrator for a jihadi forum endorsed by the Taliban wrote in a post that the "group's main site and the site of its online journal Al-Sumud, have been the subject

of an 'infiltration operation,' " according to Wired.com. The post goes on to warn online jihadists "to not enter any of the links that concern these websites, and not even to surf [the content] until you receive the confirmed news by your brothers, Allah-willing." Outages of jihadist Web sites are relatively common, though this may be the first example on a site being hacked, a spokesman of Flashpoint Partners told Wired. While no one has claimed credit for the hack, the Department of Defense has previously announced its intentions to take-down terrorist affiliated Web sites. Source: http://www.thenewnewinternet.com/2010/06/14/taliban-hacked-dod-starts-cyber-offensive/

National Monuments and Icons

(North Carolina) **Train spills 3,000 gallons of fuel near Pisgah National Forest.** A derailed train spilled 3,000 gallons of diesel fuel near Pisgah National Forest in Old Fort, North Carolina June 17. Norfolk Southern officials said they were working to mitigate the environmental damage from the morning spill, and they are still trying to determine the cause of the accident. The derailment happened at about 5:40 a.m. in the Mill Creek area eight miles west of Old Fort in McDowell County. No one was injured and no hazardous materials besides the fuel were involved. Source: http://www.citizen-times.com/article/20100618/NEWS/306180036

(California) **ATF offers a reward of $5,000 for information regarding explosives theft.** The Special Agent in Charge of the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), San Francisco Field Division and an official with the Siskiyou County Sheriff's Office announced June 17 that ATF will offer a reward of $5,000 for information leading to the arrest and conviction of those responsible for the theft of explosives that occurred at a United States Department of Agriculture (USDA) Forest Service Site, Shasta-Trinity National Forest in Mount Shasta, California, sometime between the dates of April 12 - April 21, 2010. Since April, 2010, the Siskiyou County Sheriff's Office and ATF have investigated the theft of the stolen explosives. Investigators said the stolen explosives included 20 Reynolds, RP-83, Exploding Bridgewire Detonators, six Dyno Nobel EZ Det Nonel detonators, and six Austin Powder Rockstar electric detonators. ATF and the Siskiyou County Sheriff's Office released photographs of the types of the stolen explosives. Source: http://www.prnewswire.com/news-releases/atf-offers-a-reward-of-500000-for-information-regarding-explosives-theft-96608859.html

(Arizona) **Violence prompts strong warning at Ariz. monument.** An increase in smuggling violence at the Sonoran Desert National Monument about 80 miles south of Phoenix, Arizona, has prompted a stronger warning to visitors about drug and immigrant traffickers passing through the public lands, officials said Tuesday. The monument and three other federal lands in Arizona already have signs warning visitors that they may encounter smugglers. But 11 new signs have recently been erected and two more were planned at the Sonoran Desert National Monument. The new signs warn visitors about speeding, smuggling vehicles, and instruct them to walk away when seeing something suspicious and avoid abandoned vehicles and backpacks because they might contain drugs stashed there by smugglers. The Bureal of Land Management's chief law enforcement ranger in Arizona said authorities felt a stronger warning was needed because the area is near where a Pinal County deputy was shot in a confrontation with marijuana smugglers in April, and where two men suspected of being involved in smuggling were fatally shot earlier this month. Signs warning visitors of smugglers have been put up in the past in southern Arizona at the Sonoran Desert National Monument, Cabeza Prieta National Wildlife Refuge, Organ Pipe Cactus National Monument, and Coronado National Forest. The new signs were erected at the Sonoran Desert National Monument's access points south

of Interstate 8 between Casa Grande and Gila Bend. While the monument is not located directly on the border, it is used as a pathway for traffickers headed to Phoenix, a busy hub for moving illegal immigrants and marijuana across the United States. Smuggling at the monument declined from 2005 through 2008 but is picking up again, officials said. Authorities said they were not telling visitors to stay out of the monument, though the new signs encourage people to use the monument's lands north of the interstate. Source: http://azcapitoltimes.com/blog/2010/06/16/violence-prompts-strong-warning-at-ariz-monument/

(Colorado; Wyoming) **Mud, wind, rotting roots prompt Forest Service warning about falling trees in Colo., Wyo.** Recent rain, melting snow, a beetle infestation and strong wind are shaping up to be a dangerous combination in the forests of Colorado and Wyoming. The U.S. Forest Service (USFS) said people should watch out for falling trees: Do not camp, park or otherwise linger beneath any of the millions of trees killed by bark beetles in recent years. A USFS spokeswoman aid the roots of those trees are rotting. Combined with muddy ground and strong winds this week, that is bringing down large numbers of trees onto roads, trails and campsites. Beetles have killed enough of the region's pine trees to cover the state of Connecticut. Forest officials estimate that well over 100,000 trees are falling down in Colorado and southern Wyoming every day this spring. Source: http://www.kdvr.com/news/sns-bc-wy--beetles-fallingtrees,0,4415336.story

(Washington) **Forest Service plans tussock moth treatments.** About 11,000 acres of the Okanogan-Wenatchee National Forestwill be treated for Douglas fir tussock moth this year. A crew of 12 people has been making daily trips to areas scheduled for treatment. They are checking the moth larvae. The larvae need to be consuming foliage so they will ingest the insecticide. Some private landowners in the area also have scheduled treatment. Source: http://www.omakchronicle.com/nws/n100616c.shtml

(Arizona) **Lightning causes several fire starts on the North Rim of Grand Canyon National Park.** A thunderstorm passed over Northern Arizona late last week resulting in three lightning-caused fires on the North Rim of Grand Canyon National Park. The fires were discovered between June 11 and June 12. Two fires, the Walla Fire, approximately 12 miles northwest of the North Rim-developed area and the Fuller Fire approximately six miles northeast of the North Rim-developed area were both suppressed at a tenth of an acre because of potential threats. The Glades Fire is approximately nine miles southeast of the North Rim-developed area. The fire is currently estimated at 1/10th of an acre – the fire is burning primarily in Ponderosa pine and is being managed for resource and protection objectives. It is located on the Walhalla Plateau one mile east of Cape Royal Road between Vista Encantada and Cape Final. This area previously burned in 1999 and 2005, reducing the potential for high severity fire due to the reduction of fuels. Four Grand Canyon firefighters are committed to the current fire. Source: http://www.nps.gov/grca/parknews/lightning-causes-several-fire-starts-on-the-north-rim-of-grand-canyon-national-park.htm

POSTAL AND SHIPPING

(Arizona) **Mayo Clinic's letter with white powder sent to FBI.** Scottsdale, Arizona police and fire have handed over a letter containing a white substance delivered to a Scottsdale hospital to the U.S. Postal Inspector and FBI for investigation, police said. The two groups will try to determine who sent the letter, which was found to be non-hazardous, a Scottsdale officer said. An employee in the mailroom

at the Mayo Clinic on 134th Street and Shea Boulevard discovered a letter that contained a white, powdery substance at 1:30 p.m. Monday. The mailroom supervisor called police. While the letter caused no injuries or evacuation, four employees were treated as a precaution, the officer said. Source: http://www.azcentral.com/news/articles/2010/06/16/20100616scottsdale-FBI-mayo-letter-abrk0616.html

(Ohio) **2 'bottle bombs' detonated near home of Oakwood school officials.** Police are asking for the public's help in finding the individuals who constructed "bottle bombs" filled with BB-gun ammunition and other chemicals that exploded outside the homes of two Oakwood Schools employees this weekend. The public safety captain said the residents of both homes in Oakwood, Ohio were sleeping, and no one was injured. One bottle exploded inside a mailbox attached to a house and the other blew up in a front yard at about 2 a.m. June 12. "This appears to be targeted because of the direct (school) relation between the two victims," a detective said. "Whoever is responsible for this went above and beyond what is normally used to create such devices. They intentionally put projectiles in the device that are capable of causing serious harm to persons or property." Materials were placed in the sealed, personal-size water bottles to create a chemical reaction, causing the bottles to explode. The first explosion occurred in the mailbox of a high school teacher's house on Fairmont Avenue. A few minutes later, a bottle exploded in the yard of the Oakwood high school athletic director located three blocks away on Oak Knoll Drive. Source: http://www.daytondailynews.com/news/crime/2-bottle-bombs-detonated-near-home-of-oakwood-school-officials-766093.html

(Washington; Idaho) **White powder envelopes traced back to Spokane.** Several envelopes containing a white powder were sent to federal offices Monday. The envelopes have been traced back to Spokane, Washington where they were postmarked. There will be an investigation as to whether the postmarks are authentic. The white powder within the envelopes has not yet been identified, nor have the motives behind why they were sent. The seven envelopes showed up at federal offices in Bellevue and Seattle, Washington, Boise and Coeur d'Alene, Idaho, and in Spokane. The envelopes were dealt with in different fashions, including the evacuation of the Boise U.S. Attorney's Office, and a lockdown of two people that came into contact with one of the envelopes in the Seattle downtown courthouse. It appears that the white powdery substance is nontoxic, but it has not been revealed what it actually is yet. All of the envelopes arrived at offices June 14, and were opened at different points of the day. KXLY of Spokane reported that authorities across the Pacific Northwest plan to continue the investigation. Source: http://www.examiner.com/x-7460-Spokane-Headlines-Examiner~y2010m6d15-White-powder-envelopes-traced-back-to-Spokane

(Wyoming) **Powder scare comes to city hall.** A powder scare shut down the Cheyenne, Wyoming clerk's office for three hours June 11. Initial tests show that the powder does not contain biological agents, such as anthrax. Around noon, a clerk's employee opened an envelope with a letter and an unknown powder substance. The employees had to stay locked in the office under quarantine for three hours as haz-mat officials kept them "as calm and as comfortable as we could" until tests were finished. The letter is at the state crime lab where officials will continue tests and try to grow cultures from the powder. The haz-mat team also evacuated three nearby offices: human resources, purchasing and risk management. Source: http://www.wyomingnews.com/articles/2010/06/12/news/20local_06-12-10.txt

PUBLIC HEALTH

J&J recalls Benadryl, Tylenol overlooked in January. Johnson & Johnson company June 15 said it has recalled four additional lots of Benadryl allergy tablets and one lot of Extra Strength Tylenol gels. The diversified healthcare company, in a press release, said it was recalling the lots after inadvertently failing to include them in a wider recall of over the counter drugs January 15. The company's McNeil Consumer Healthcare unit said the latest action is a "follow-up" to the recall in January. On that occasion, 53 million bottles of a range of products were recalled after consumers complained of musty or moldy odors. The brands included Tylenol and Motrin painkillers, Rolaids, Benadryl, and St. Joseph's Aspirin. The drugmaker said the odor that prompted its January 15 recall was linked to traces of a chemical called TBA, caused by the breakdown of a chemical applied to wood used to build pallets that transport and store product-packaging materials. "Further analysis confirms that the risk of serious adverse medical events is remote," J&J said June 15. J&J said the newly recalled lots — made at a plant in Las Piedras, Puerto Rico — were sold in the United States, Trinidad and Tobago, Bermuda, and Puerto Rico. One of McNeil's two other main factories, located in Ft. Washington, Pennsylvania, has been shut down while the company strives to fix multiple deficiencies cited by the U.S. Food and Drug Administration. Source: http://www.reuters.com/article/idUSTRE65E67020100615?type=domesticNews

Infected organs pose deadly transplant risk. The patient was 54 when he died in 2005 after receiving a kidney that was infected with a rare virus from the donor's pet hamster. He endured more than three years of dialysis waiting for a new kidney, even turning down one organ on his doctor's advice because it came from a high-risk donor, his wife said. But in May 2005, less than a month after the 54-year-old Rhode Island man received the long-awaited organ, he was dead, felled by a rare infection that lurked undetected in the transplanted kidney. The source? A pet hamster bought the month before the organ donor's sudden death. It was a diseased rodent whose virus, lymphocytic choriomeningitis — known as LCMV — was transmitted from the donor to four people who received her organs, killing three of them. The fourth became critically ill, but survived. Last month, that victim and the families of the others settled a two-year lawsuit against the retailer PetSmart, who they claimed failed to screen the sick hamster or to warn pet owners about potential dangers. Source: http://www.newsvine.com/_news/2010/06/11/4495780-infected-organs-pose-deadly-transplant-risk

(Massachusetts) **Nahant man, pal nabbed at Bedford hospital with bomb.** A Nahant, Massachusetts man was arrested after he allegedly handed over a homemade pipe bomb to police outside the Bedford Hospital late Friday. The Nahant man, and another man of Salem, were taken into custody after police approached the two for acting suspiciously. Both are expected to be arraigned June 15. According to a Bedford police sergeant, the two men arrived at the Edith Nourse Rogers Memorial Veterans Hospital, where one of the men was planning to attend a detox program. He said the two had been walking near the emergency department and were pointing at several nearby buildings, when hospital officials detained them. The Salem man was found to have an outstanding warrant issued out of Salem for operating under the influence and drug charges. However, as police were arresting the Salem man, they looked into the suspects' vehicle and saw an open container of alcohol and began questioning the Nahant man. Police say he then handed over a pipe bomb and marijuana. Source: http://www.thedailyitemoflynn.com/articles/2010/06/14/news/news06.txt

Americans get most radiation from medical scans. Americans get the most medical radiation in the world, even more than folks in other rich countries. The U.S. accounts for half of the most advanced procedures that use radiation, and the average American's dose has grown sixfold over the last couple of decades. Too much radiation raises the risk of cancer. That risk is growing because people in everyday situations are getting imaging tests far too often. Doctors don't keep track of radiation given their patients — they order a test, not a dose. Except for mammograms, there are no federal rules on radiation dose. Children and young women, who are most vulnerable to radiation harm, sometimes get too much at busy imaging centers that don't adjust doses for each patient's size. That may soon change. In interviews with The Associated Press, U.S. Food and Drug Administration (FDA) officials described steps in the works, including possibly requiring device makers to print the radiation dose on each X-ray or other image so patients and doctors can see how much was given. The FDA also is pushing industry and doctors to set standard doses for common tests such as CT scans. A near-term goal: developing a "radiation medical record" to track dose from cradle to grave. "One of the ways we could improve care is if we had a running sort of Geiger counter" that a doctor checked before ordering a test, said a Duke University physician. He led an eye-opening study that found that U.S. heart attack patients get the radiation equivalent of 850 chest X-rays over the first few days they are in the hospital — much of it for repeat tests that may not have been needed. Source: http://www.google.com/hostednews/ap/article/ALeqM5hkPUKD008bd8xhXg2HtRmnv0dbvwD9GAQIPO0

Ray technology could detect bioterror agents. Terahertz ray technology could be used to detect traces of disease spores like smallpox or explosive materials at security checkpoints, the Newark, N.J., Star-Ledger reported June 13. The technology is an example of research being conducted at the New Jersey Homeland Security Technology Systems Center at the New Jersey Institute of Technology. "High-tech, low-tech, we can't afford to overlook any possibility in dealing with mass casualty events," according to the head of the center. Terahertz rays operate on a separate bandwidth from their counterparts X-rays and microwaves. A physicist said they could be used to check people for dangerous materials to parts per billion trace levels without any threat of dangerous radiation, the Star-Ledger reported. Scanners emitting the rays could quickly identify someone trying to carry even minutes amounts of a bioterrorism agent such as anthrax or smallpox into a secure area. The physicist is working on an efficient use of the technology coupled with digital video to read the scans, which could see through cardboard, walls, packages, pill capsules, clothing and shoes. Source: http://www.globalsecuritynewswire.org/gsn/nw_20100614_3990.php

TRANSPORTATION

(North Carolina) **Charlotte train station evacuated, bomb squad called out.** A Charlotte, North Carolina Amtrak station was evacuated June 17 after a suspicious item was found on a train. An Amtrak spokeswoman said Norfolk Southern police asked them to evacuate the entire facility after the suspicious items were found on top of three tankers aboard a train around 10:30 a.m. Thursday. Police officers and the bomb squad were called to the Charlotte Amtrak station to help in the investigation. The affected train was Train 73 from Raleigh to Charlotte, which had 47 passengers on board. Source: http://www.wmbfnews.com/Global/story.asp?S=12665844

FAA experiments with integrating drones in civil airspace. The Federal Aviation Administration (FAA) is studying how to integrate unmanned aerial vehicles (UAVs) into U.S. airspace alongside conventional aircraft. Although UAVs have been flying in the United States for several years, they are limited to restricted airspace as well as portions of the borders with Canada and Mexico. The problem of operating unmanned aircraft within the same airspace as conventional aircraft has been a contentious issue for pilots and carriers. Under an agreement the FAA signed last week with Boeing subsidiary Insitu, the feds will begin flying an unmanned aircraft as part of continuing research using air traffic control simulations. Insitu will provide the FAA with a ScanEagle unmanned aircraft system for the research, which will be conducted at the William J. Hughes Technical Training Center in Atlantic City, New Jersey. The goal is to evaluate how an air traffic controller can manage unmanned aircraft along with manned aircraft. The ScanEagle is a relatively small UAV with a 10-foot wingspan. It weighs less than 50 pounds. During the research program, the New Jersey National Guard will fly the UAV within current air traffic control simulations operating in a restricted airspace. Other UAV makers, including General Atomics, maker of the larger Predator family of unmanned aircraft, have similar agreements with the FAA. Unmanned aircraft do not currently fly within U.S. airspace except within a handful of restricted regions or with a special waiver. Versions of the General Atomics Predator have been flying border patrols for a few years now, even operating from airports with a mix of small general aviation aircraft. Source: http://www.wired.com/autopia/2010/06/faa-uav-civil-airspace/

(Oklahoma) **Okla. flash floods strand cars, close interstates.** Flash flooding across Oklahoma City stranded motorists on their morning commutes Monday, prompting at least a half-dozen rescues and three interstate closures, authorities said. No injuries were immediately reported but drivers were being warned to stay home, an Oklahoma Police lieutenant said. Portions of interstates 35, 44 and 235 all were closed, as were numerous smaller roads in and out of the metro area. Lightning knocked out electricity to some areas. “Downtown is flooded,” the Oklahoma City spokeswoman said. “We have a few traffic lights that are out causing problems. Stalled vehicles are causing problems. Crews are in the same situation that our travelers are in. They are stuck in this traffic as well.” Source: http://www.msnbc.msn.com/id/37687237/ns/weather/?GT1=43001

Water and Dams

EPA proposes updating drinking water rule to better protect public health. The U.S. Environmental Protection Agency (EPA) is proposing to revise a national primary drinking water regulation to achieve greater public health protection against waterborne pathogens in the distribution systems of public water systems. EPA is proposing to revise the 1989 Total Coliform Rule to incorporate improvements recommended by a federal advisory committee. The revised rule will better protect people from potential exposure to dangerous microbes because it requires water systems to take action when monitoring results indicate that contamination or a pathway to contamination may be present. The proposal also provides incentives for better system operation by improving the criteria for public water systems to qualify for and stay on reduced monitoring, which provides an opportunity to reduce system burden. In addition, the proposed rule updates conditions that will trigger public notices to better represent the relative health threat identified. It also makes the wording required in these public notices more clear. EPA is seeking public comment on this proposed rule for 60 days following publication in the Federal Register. Source: http://yosemite.epa.gov/opa/admpress.nsf/0/2E4503668A34B3DD852577450061A0C8

Federal study finds streams easily hurt by development. New houses and businesses that spring up along the edges of cities always have posed a pollution threat to wildlife in nearby streams. But a new study by the U.S. Geological Survey that examined more than 250 streams that flow near nine major cities found that aquatic life declines almost as soon as new roads and buildings go up. Experts had thought that the decline began much later, after pavement and buildings filled at least 10 percent of open land near streams. Even at that 10-percent level, as much as 36 percent of the aquatic insects that form the base of streams' food chains already were destroyed by stormwater and dirt from eroded stream banks, the study found. Instead of sinking into the ground, rain falls on roofs, roads and pavement and quickly flows into storm drains and streams. When storms hit, the fast-moving water erodes stream banks and carries with it lawn fertilizers, pesticides and pollutants cars leave on pavement. Government officials said safeguards for streams must be given a chance to work. That would mean several years of monitoring and testing streams. Source: http://www.dispatch.com/live/content/local_news/stories/2010/06/14/federal-study-finds-streams-easily-hurt.html?sid=101

(Nebraska) **Dam failure forces evacuation of Nebraska town.** Heavy rain and storm runoff that swelled creeks and rivers briefly threatened a small hospital and forced the evacuation of a small town in central Nebraska Saturday, officials said. North Loup, a town of about 340 in central Nebraska's Valley County, was evacuated because of street flooding that followed failure of a small dam, state officials said. A sheriff's dispatcher said no injuries had been reported. Radio station KNLV in Ord said a shelter for North Loup residents was being arranged in nearby Scotia. The sheriff said residents would be allowed to return to town Saturday night once electricity and gas lines were checked and repaired. He said the floodwater was deepest — up to 4 feet — on the north side of town. A few basements had fallen in, he said, and floodwaters caused sewer problems. He said an earthen dam holding back a private pond gave way and sent water down Mira Creek, which flows along the north side of town. Source: http://www.siouxcityjournal.com/news/state-and-regional/nebraska/article_a3017108-7699-11df-a371-001cc4c002e0.html

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: Fusion Center (24/7): 866-885-8295(In ND only); Email: ndslic@nd.gov ; Fax: **701-328-8175**
State Radio: 800-472-2121 Bureau of Criminal Investigation: 701-328-5500 Highway Patrol: 701-328-2455
US Attorney's Office Intel Analyst: 701-297-7400 Bismarck FBI: 701-223-4875 Fargo FBI: 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, **701-328-8168**